

## Claims

What is claimed is:

1. A system for managing communications between one or more on-board modules associated with a work machine and connected to one or more on-board data links and one or more off-board systems connected to one or more off-board data links, the system comprising:

a first off-board system connected to a first off-board data link, wherein the off-board module is remotely located from the work machine; and

a gateway embedded in the work machine including:

a communication application that uses a translation table stored in the gateway for converting information from a first protocol format to a second protocol format, and

a firewall application that is configured to perform, when executed by a processor, a firewall process that controls access to proprietary information associated with the work machine,

wherein the firewall process determines whether a message received from the first off-board system is authorized based on a profile associated with the first off-board system, whether a message received from the first off-board module includes a parameter identifier corresponding to one of a number of parameter identifiers included in the translation table, and denies access to the proprietary information based on at least one of (i) a determination that the parameter identifier in the data message does not correspond to one of the number of parameter identifiers in the translation table and (ii) the profile associated with the off-board system.

2. The system of claim 1, wherein the firewall process denies or grants access to the proprietary information based on a profile associated with a user operating the first off-board system.

3. The system of claim 1, wherein the profile is associated with a user of the off-board system and defines a type of access to a selected portion of the proprietary information.

4. The system of claim 1, wherein the proprietary information includes a parameter identifier data value.

5. The system of claim 1, wherein the firewall process allows the first off-board system to access the proprietary information when the parameter identifier in the message matches at least one parameter identifier included in the translation table.

6. The system of claim 5, wherein the gateway executes the communication application to convert the request to a different protocol format when the firewall process allows the off-board system to access the proprietary information.

7. The system of claim 1, wherein the firewall process denies access to an on-board module based on parameter information included in a second message.

8. The system of claim 1, wherein the work machine moves between, or within, a work environment and the firewall application controls access to proprietary information located in a remote location based on the position of the work machine.

9. The system of claim 8, wherein the gateway receives the message from a second gateway included in the second work machine that has moved into communication range of the work machine.

10. The system of claim 1, wherein the firewall application performs a second firewall process that controls access to the proprietary information based on a timing profile associated with the type of request.

11. The system of claim 1, wherein the request is a batch request including multiple sub-requests associated with the proprietary information, and the firewall process denies access to a portion of the proprietary information based on a determination that parameter identifiers associated with a respective portion of the sub-requests do not match any of the parameter identifiers included in the translation table.

12. A method for managing communications in an environment including a work machine having one or more on-board data links connected to one or more on-board modules and a gateway, and one or more off-board data links connected to one or more off-board systems and the gateway, the method performed by the gateway comprising:

receiving a request generated by a first off-board system and transmitted on a first off-board data link; and

invoking a firewall application that performs a firewall process including the steps of:

identifying a destination device associated with the request,

determining whether the request is authorized based on a profile associated with the first off-board system,

determining whether the request includes a parameter identifier that matches a parameter identifier included in a memory location maintained by the gateway, and  
denying or granting access to proprietary information based on the two determining steps.

13. The method of claim 12, wherein the profile is associated with a user of the off-board system and defines a type of access to a selected portion of the proprietary information.

14. The method of claim 12, wherein the proprietary information includes a parameter identifier data value.

15. The method of claim 12, wherein the firewall process allows the first off-board system to access the proprietary information when the parameter identifier in the request matches at least one parameter identifier included in the memory location.

16. The method of claim 12, wherein the gateway executes a communication application to convert the request to a different protocol format when the firewall process allows the off-board system to access the proprietary information.

17. The method of claim 16, wherein the memory location is included in a translation table used by the communication application to convert parameter data values to different formats.

18. The method of claim 12, wherein the firewall process denies access to an on-board module based on parameter information included in a second request.

19. The method of claim 16, wherein the work machine moves between, or within, a work environment and the method further includes:  
controlling access to proprietary information located in a remote location based on the position of the work machine.

20. The method of claim 19, wherein the gateway receives the request from a second gateway included in a second work machine that has moved into communication range of the work machine.

21. The method of claim 12, wherein the method further includes:  
controlling access to the proprietary information based on a timing profile associated with the type of request.

22. The method of claim 12, wherein the request is a batch request including multiple sub-requests associated with the proprietary information, and the firewall process further includes:  
denying access to a portion of the proprietary information based on a determination that parameter identifiers associated with a respective portion of the sub-requests do not match a parameter identifier included in the memory location.

23. A computer-readable medium including instruction for performing, when executed by a processor, a method for managing communications in an environment including a work machine having one or more on-board data links connected to one or more on-board modules and a gateway, and one or more off-board data links connected to one or more off-board systems and the gateway, the method performed by the gateway comprising:

receiving a request generated by a first off-board system and transmitted on a first off-board data link; and

invoking a firewall application that performs a firewall process including the steps of:

identifying a destination device associated with the request,

determining whether the request is authorized based on a profile associated with the first off-board system,

determining whether the request includes a parameter identifier that matches a parameter identifier included in a memory location maintained by the gateway, and

denying or granting access to proprietary information based on the two determining steps.